El software de las máquinas de votación pasa la prueba

Tiempo de lectura: 8 min.

Observatorio Electoral Venezolano

Lun, 04/10/2021 - 08:56

El Observatorio Electoral Venezolano (OEV) comparte con los electores las notas de nuestra observación a la auditoría de software de la máquina de votación rumbo al 21-N. De la revisión se desprende que funciona bien, es seguro y está configurado para que el voto sea secreto, y, sobre todo, auditable, con amplias herramientas para hacerlo

La auditoría del software de la máquina de votación se celebró del 30 de agosto al 10 de septiembre. Representantes de partidos políticos y de organizaciones de la sociedad civil realizaron durante estos días el proceso de observación y levantamiento de información del estado general de las aplicaciones que conforman el sistema automatizado de votación, configurado para las elecciones regionales y municipales de noviembre de 2021.

El Consejo Nacional Electoral (CNE) invitó al OEV a observar esta auditoría a través de plataformas virtuales. En esta nota presentamos a los electores un resumen de las anotaciones y conclusiones a las cuales llegó nuestra observadora Ana Morales Bezeira, profesora de la Escuela de Computación en la Facultad de Ciencias de la Universidad Central de Venezuela (UCV).

La profesora Morales es doctora en Ciencias de la Computación, mención Redes. Es jefa del Centro de Investigación de Comunicaciones y Redes (CICORE) y coordinadora del Laboratorio de Redes Móviles, Inalámbricas y Sistemas Distribuidos (ICARO) en la UCV.

El proceso de auditorías consistió en la revisión detallada de cinco softwares que conforman la estructura del sistema automatizado de votación. Ellos son:

Módulo de transmisión (ContingencyTransmissionTool).

Módulo de protección y seguridad de los datos electorales (DataProtector).

Módulo SAI (SAIUnlock).

Módulo de captura y validación de huellas dactilares (SessionLogsAndFingerprintsValidator).

Software de máquina de votación (VotingMachine).

El proceso de auditorías partió desde los archivos hash resultantes como definitivos del proceso de auditoría integral al sistema automatizado de votación realizada por 10 académicos, de reconocida competencia en estas materias, entre junio y julio, de la cual surgieron un conjunto de observaciones y modificaciones.

¿Y qué es un archivo hash? Es una especie de firma digital que se hace para proteger los archivos de un software. Es el resultado de una técnica compleja, que arroja un código único. Si se hiciera una nueva modificación a los archivos del

software, este código ya no coincidiría.

Así, la auditoría integral de los académicos arrojó al final un código. Este fue recibido por los participantes de la auditoría del software, certificando que no hubo cambios al sistema entre esa fecha y esta. Luego de las respectivas mejoras de esta auditoría se generó otro código, que usarán los participantes de la auditoría de producción de máquinas, a partir del 26 de octubre.

Estos son 10 de los aspectos observados, en orden cronológico durante la auditoría, y algunas oportunidades de mejora resultantes de nuestra observación:

1.En la auditoría se mostró cómo las bases de datos en la máquina de votación se encuentran vacías, así como las validaciones de inicialización que hace el software de las máquinas al momento de su instalación. Esto se hace con la finalidad de garantizar que no existan registros previos de procesos de votación en esas bases de datos.

¿Qué significa lo anterior? que la máquina al inicio del proceso de votación empieza vacía, con cero votos, como es debido.

2.Se observó en la auditoría que, al momento del proceso de inicialización e instalación de las máquinas de votación, no se registra ni se valida la identidad de los miembros que abren la mesa.

Al respecto, los técnicos señalaron que ese registro se realiza de manera manual. Solo al final de la jornada electoral, cuando ya se cierra la mesa y la máquina de votación, es cuando el sistema permite agregar miembros de mesa para generar e imprimir el acta de escrutinio y cierre de la mesa.

Sobre este particular, el OEV sugiere que la carga de la información de identidad de los miembros de mesa en cada máquina también se podría realizar manejando una base de datos de miembros de mesa, ya que esta es una información que se conoce de manera anticipada al día de la votación. Esta sugerencia debe entenderse como una oportunidad para agregar valor al sistema; la manera como se hace ahora, sin embargo, no pone en riesgo el proceso.

3.En la auditoría se observó que, una vez instalada una máquina de votación, no es posible cambiar o modificar los archivos de su base de datos, ni los archivos de los electores de una máquina.

Es esta una garantía favorable para los electores.

4.Se observó que el tiempo máximo que tiene un votante de interactuar con el sistema de votación durante el proceso de selección de sus candidatos es de tres minutos; transcurrido ese tiempo el sistema de manera automática genera e imprime un voto nulo.

Se sugirió que se incremente este lapso a por lo menos cinco minutos, ya que el proceso electoral 2021 resulta complejo para el votante, y de muchas selecciones (se elegirán gobernadores, legisladores, alcaldes y concejales el mismo día), sobre todo si es decisión del elector hacer un voto cruzado (por más de una tarjeta). Los técnicos indicaron que se elevaría esa sugerencia a las autoridades del CNE.

5.En esta auditoría se presentaron observaciones y comentarios referentes a la forma en que son presentadas las opciones de voto a los electores. Esto, en palabras técnicas, se refiere a la interfaz de experiencia de usuario, partiendo de la interfaz principal con la tarjeta electoral en la cual salen todos los partidos, que llamaremos interfaz 1 para fines explicativos.

En la experiencia del voto, primero se debe seleccionar una tarjeta de un partido político; es decir, se ata todo el voto a esta primera selección. Luego, se va a la interfaz en la que se observan dos secciones: gobernador y consejos legislativos; y alcaldes y concejos municipales, del partido ya seleccionado. Si esto continúa así, se estaría entubando el voto.

Hacer un voto cruzado sí se podría técnicamente, pero resulta complejo para el elector: estando en la segunda interfaz le correspondería al votante deseleccionar alguna opción de voto, y volver atrás a la primera interfaz para realizar otras selecciones individualizadas de otra(s) tarjeta(s) de partidos políticos hasta completar su votación para todos los cargos.

6.Se explicó durante la auditoría las partes del código del software que se encargan de almacenar el voto en la base de datos. Una certeza: el orden en el que los votos se almacenan es aleatorio. Esto se hace con la finalidad de impedir el rastreo de sufragios en el mismo orden en el que lo realizan los votantes, y evitar asociar un voto de manera directa a un votante en particular, según su orden de votación.

¿Qué significa esto? que queda descartado el mito de que tecnológicamente la máquina revele por quién votó una persona en particular. No hay relación posible

entre un elector y su opción de voto.

7.El sistema lleva un registro de los tiempos de votación empleados por cada usuario. Esto con la finalidad de, en el futuro, tener una mayor información del tiempo promedio que toma a los votantes interactuar con el sistema. Esta mejora es producto de la auditoría integral cumplida por 10 académicos venezolanos en meses anteriores.

8.En la auditoría se indicó que el acta incluye un código QR con información del escrutinio. Esta información puede ser utilizada por los partidos políticos para sus propias estadísticas e información requerida a través de aplicaciones desarrolladas de manera particular por las organizaciones.

¿Esto es positivo? sí, porque contribuye a la trazabilidad de los resultados e incrementa la trasparencia.

9.El representante de la MUD preguntó si al momento de la transmisión se vuelve a realizar un recálculo de los escrutinios. Se aclaró en la auditoría que no. Una vez realizados los escrutinios y creada el acta, momento en el cual se hacen los cálculos de resultados del proceso, este procedimiento de cálculos no se vuelve a realizar. La transmisión se hace únicamente con el paquete que se construye a partir de los escrutinios ya calculados una vez que se cierra la mesa de votación.

¿Que no se haga este recálculo es positivo? Sí; y también da certezas sobre la seguridad en la fase de transmisión de los votos.

10. El procedimiento a seguir en los casos de las personas con ausencia de miembros superiores, o problemas en las manos y ausencia de huellas es con asistencia e intervención del presidente de la mesa, quien debe intervenir utilizando su clave especial y sus huellas dactilares.

Finalmente, como resultado de la auditoría al software de la máquina de votación, el cuerpo técnico del CNE hizo mejoras y modificaciones al software final. El conjunto de modificaciones realizadas se resume en:

a) Cambios en los métodos de generación de claves, tanto las de los entes representantes del CNE, como para la generación de claves de los representantes de los partidos políticos. Asimismo, se asoció a cada clave el nivel de acceso (administrador, partido político…) al que pertenece. De igual forma, se modificó el

código para que cada máquina de votación manejase una clave única.

En resumen, todo esto es positivo desde el punto de vista de la seguridad del sistema.

b) Cambios en el método que gestiona la lista de no duplicidad en las máquinas de votación.

¿Qué es la lista de no duplicidad? Es una suerte de “cola” en donde se almacena de manera aleatoria la huella de cada elector una vez que su proceso de votación se completa. ¿Y para qué se genera esa cola? Para garantizar que si luego el mismo elector pretende volver a votar, lógicamente con su huella, el sistema no se lo permita.

¿Cómo era antes? Solo se registraban las huellas que se captaban y validaban satisfactoriamente. ¿Por qué con el cambio ahora es mejor? Porque se incluyen también todas aquellas huellas captadas del votante (es decir, las llamadas “no match”; las borrosas o difíciles de identificar), almacenando no solo las ya enroladas en el sistema, sino las de nueva captura.

Se aclara aquí que las huellas en la lista de no duplicidad se almacenan de manera aleatoria; es decir, no coinciden con el orden en el que se registran las opciones de voto seleccionadas. Esto da garantías para el secreto del voto.

c) Se agregó en el acta impresa de escrutinios la fecha y hora de apertura, y hora de cierre de cada mesa.

En resumen, luego de conocer el informe y la valoración técnica de nuestra observadora en esta auditoría, podemos concluir que el software de la máquina de votación funciona bien y es seguro. Está configurado para que el voto sea secreto, se cuente y transmita bien y, sobre todo, sea auditable; en este sentido, los actores participantes disponen de buenas herramientas para hacerlo. El mismo sistema ofrece amplias oportunidades de auditabilidad que permiten detectar cualquier alteración o irregularidad en los procesos de votación, conteo y totalización.

Boletín 71

Septiembre de 2021

https://oevenezolano.org/2021/09/boletin-71-el-software-de-las-maquinas-...

ver PDF

Copied to clipboard